AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method for modeling a behavior of normal users in a network in response to an application of a first filtering technique, comprising:

receiving a group of packets from a first user subsequent to the application of the first filtering technique;

associating at least one feature with each packet in the group of packets,

associating at least one annotation with the at least one feature, the at least one annotation including an annotation identifying the first filtering technique and

creating at least one model reflecting a behavior of the first user based on the features associated with the group of packets.

2. (Original) The method of claim 1 wherein the at least one model includes Hidden Markov Models.

3. (Cancelled)

4. (Previously Presented) The method of claim 1 wherein the at least one feature includes at least one of packet types, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

5. (Canceled)

6. (Currently Amended) The method of claim [[5]] 1,further comprising:

storing the at least one feature and associated at least one annotation.

7. (Currently Amended) The method of claim [[5]] 1 further comprising:

verifying an accuracy of the at least one model using the stored at least one feature and associated at least one annotation.

8. (Cancelled)

9. (Original) The method of claim 1 further comprising:

applying a different filtering technique;

receiving additional packets from the first user after applying the different filtering technique; and

creating additional models reflecting the behavior of the first user based on the additional packets.

10. (Original) The method of claim 1 wherein the receiving includes:

receiving a stream of packets from a plurality of users,

identifying the packets in the stream to obtain identified first user packets, and

grouping said identified first user packets.

11. (Currently Amended) A system for modeling normal user behavior in a network, comprising:

a memory configured to store instructions; and

a processor configured to execute the instructions to:

filter packets in the network using a first filtering technique,

receive a group of packets from a first user after the filtering,

associate at least one feature with each packet in the group,

associate at least one annotation with the at least one feature, the at least one annotation including an annotation identifying the first filtering technique, and

create at least one model reflecting a behavior of the first user based on the features associated with the group of packets.

12. (Original) The system of claim 11 wherein the at least one model includes Hidden Markov Models.

13. (Cancelled)

14. (Previously Presented) The system of claim 11 wherein the features include at least one of packet types, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

15. (Canceled)

16. (Currently Amended) The system of claim [[15]] 11 wherein the processor is further configured to:

store the at least one feature and associated at least one annotation in the memory.

17. (Currently Amended) The system of claim [[15]] 11 wherein the processor is further configured to:

verify an accuracy of the at least one model using the stored at least one feature and associated at least one annotation.

18. (Cancelled)

19. (Original) The system of claim 11 wherein the processor is further configured to:

apply, after creating the at last one model, a second filtering technique,

receive a subsequent group of packets from the first user after applying the second filtering technique, and

create additional models reflecting the behavior of the first user in response to the second filtering technique.

20. (Original) The system of claim 11 wherein, when receiving the group of packets, the processor is configured to:

receive a stream of packets from a plurality of users,

identify the packets in the stream, and

group packets from the first user.

21. (Currently Amended) A computer-readable medium containing instructions for controlling at least one processor to perform a method for modeling a behavior of users in a network in response to an application of a first filtering technique, comprising:

receiving, subsequent to the application of the first filtering technique, a number of packets from a first user;

associating at least one feature with each packet in the received packets

associating at least one annotation with the at least one feature, the at least one annotation including an annotation identifying the first filtering technique; and

creating at least one model reflecting a behavior of the first user based on the features associated with the received packets.

22. (Original) The computer-readable medium of claim 21 wherein the at least one model includes Hidden Markov Models.

23. (Previously Presented) The computer-readable medium of claim 21, wherein the at least one feature includes at least one of packet types, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

24. (Original) The computer-readable medium of claim 21 wherein the receiving includes:

receiving a stream of packets from a plurality of users, and

grouping packets associated with the first user.

25. (Currently Amended) A method for protecting against network attacks that includes detecting an attack and applying a filtering technique, comprising:

receiving, subsequent to the filtering technique being applied, a stream of packets;

identifying each packet in the stream;

associating at least one feature with each packet;

partitioning the packets into groups, each group corresponding to a plurality of packets;

identifying, for each group of packets, at least one model from a plurality of previously created models, ~~classifying each group of packets as a normal group or an attack group using at least one model,~~ each model reflecting a normal response to an application of the filtering technique;

comparing the features associated with a group of packets with features of each of the at least one identified model,

generating a closeness score for each of the at least one identified model based on the comparing,

determining whether the closeness score for each of the at least one identified model equals or exceeds a threshold, and

identifying the group of packets as a normal group when the closeness score of at least one of the identified models equals or exceeds the threshold,

allowing the normal groups to pass on toward their destination; and

filtering groups of packets classified as attack groups using the filtering technique.

26. (Canceled)

27. (Currently Amended) The method of claim [[26]] 25 wherein the features include at least one of at least one type of packets, characteristics of packet headers, time between similar packets, and characteristics of packet loads.

28. - 29 (Canceled)

30. (Original) The method of claim 25 wherein the at least one model includes Hidden Markov Models.

31. (Original) The method of claim 25 wherein the at least one model relates to the filtering technique.

32. (Currently Amended) A system for identifying normal traffic during a network attack, comprising:

means for receiving, subsequent to a filtering technique being applied, a stream of packets;

means for identifying each packet in the stream;

means for associating at least one feature with each packet;

means for partitioning the packets into groups, each group corresponding to a plurality of packets;

means for identifying, for each group of packets, at least one model from a plurality of previously created models, ~~classifying each group of packets as a normal group or an attack group using at least one model,~~ each model reflecting a normal response to an application of the filtering technique;

means for comparing the features associated with a group of packets with features of each of the at least one identified model,

means for generating a closeness score for each of the at least one identified model based on the comparing,

means for determining whether the closeness score for each of the at least one identified model equals or exceeds a threshold,

means for identifying the group of packets as a normal group when the closeness score of at least one of the identified models equals or exceeds the threshold,

means for allowing groups of packets classified as normal groups to pass on toward their destination, and

means for filtering groups of packets classified as attack groups using the first filtering technique.

33. (Currently Amended) A system for identifying normal traffic during a network attack, comprising:

a memory configured to store a plurality of models, each model reflecting a normal response to an application of a filtering technique; and

a processor connected to the memory and configured to:

receive a stream of packets subsequent to a first filtering technique being applied,

identify each packet in the stream;

associate at least one feature with each packet;

partition the stream into strands, each strand corresponding to a plurality of packets,

identify, for each group of packets, at least one model from a plurality of previously created models, ~~classify each group of packets as a normal group or an attack group using at least one model,~~ each model reflecting a normal response to an application of the filtering technique;

compare the features associated with a group of packets with features of each of the at least one identified model,

generate a closeness score for each of the at least one identified model based on the comparing,

determine whether the closeness score for each of the at least one identified model equals or exceeds a threshold,

identify the group of packets as a normal group when the closeness score of at least one of the identified models equals or exceeds the threshold,

allow strands classified as normal strands to pass on toward their destination, and

filter strands classified as attack strands using the first filtering technique.

34-35 (Cancelled)

36. (Previously Presented) The system of claim 33 wherein, when partitioning, the processor is configured to:

group packets in the stream based on a source of the packets.

37–38. (Cancelled)

39. (Currently Amended) The system of claim [[38]] 33 wherein the at least one identified model includes models associated with the first filtering technique.

40. (Original) The system of claim 33 wherein the plurality of models include Hidden Markov Models.

41. (Currently Amended) A computer-readable medium containing instructions for controlling at least one processor to perform a method for identifying normal traffic during a network attack, comprising:

receiving, subsequent to an application of a first filtering technique, a stream of packets;

grouping packets in the stream based on at least a source of the packets;

associating, prior to grouping, at least one feature with each packet in the stream of packets,

identifying, through the use of Hidden Markov Models (HMMs), each packet group as a normal group or attack group, the HMMs representing normal responses to the application of the first filtering technique, wherein identifying includes,

identifying, for each packet group, at least one HMM from a plurality of previously created HMMs,

comparing the features associated with a packet group with features of each of the at least one HMMs,

generating a closeness score for each of the at least one HMMs based on the comparing,

comparing each closeness score to a threshold,

identifying the packet group as a normal group when at least one of the closeness scores equals or exceeds the threshold, and

allowing groups of packets identified as normal groups to pass on toward their destination, and

filtering packet groups classified as attack groups using the first filtering technique.

42-56. (Cancelled)